Attorney Docket No.: BHT-3111-382

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	:	
Chih-Pen CHANG, et al.	:	Group Art Unit: 2183
Application No.: **10/721,289**	:	Examiner: Not Yet Assigned
Filed: November 26, 2003	:	
For: **SPEED-UP HARDWARE ARCHITECTURE FOR CCMP ENCRYPTION PROTOCOL**	:	

CLAIM TO PRIORITY UNDER 35 U.S.C. § 119

Assistant Commissioner of Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Sir:

Pursuant to the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55, Applicant claims the right of priority based upon **Taiwanese Patent Application No. 092115621 filed June 10, 2003.**

A certified copy of Applicant's priority document is submitted herewith.

Respectfully submitted,

By: 
Bruce H. Troxell
Reg. No. 26,592

TROXELL LAW OFFICE PLLC
5205 Leesburg Pike, Suite 1404
Falls Church, Virginia 22041
Telephone: (703) 575-2711
Telefax: (703) 575-2707

Date: March 26, 2004

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder :

申　　請　　日 ： 西元 2003 年 06 月 10 日
Application Date

申 請 案 號 ： 092115621
Application No.

申　　請　　人 ： 揚智科技股份有限公司
Applicant(s)

SN 10/721,289
AU 2183

局　　長
Director General

蔡練生

發文日期： 西元 2003 年 11 月 13 日
Issue Date

發文字號： 09221148980
Serial No.

申請日期：	IPC分類
申請案號：	

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中文	一種運用在無線加解密運算的硬體加速裝置
	英文	
二、發明人(共2人)	姓名(中文)	1. 張志鵬 2. 賴明祥
	姓名(英文)	1. 2.
	國籍(中英文)	1. 中華民國 TW 2. 中華民國 TW
	住居所(中文)	1. 台北縣板橋市溪生東路279巷12弄16-2號 2. 新竹市東區東南街289號
	住居所(英文)	1. 2.
三、申請人(共1人)	名稱或姓名(中文)	1. 揚智科技股份有限公司
	名稱或姓名(英文)	1.
	國籍(中英文)	1. 中華民國 TW
	住居所(營業所)(中文)	1. 台北市內湖路一段246號2樓 (本地址與前向貴局申請者相同)
	住居所(營業所)(英文)	1.
	代表人(中文)	1. 呂理達
	代表人(英文)	1.

申請日期：	IPC分類
申請案號：	

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中 文	一種運用在無線加解密運算的硬體加速裝置
	英 文	
二、發明人(共2人)	姓 名(中文)	1. 張志鵬 2. 賴明祥
	姓 名(英文)	1. 2.
	國 籍(中英文)	1. 中華民國 TW 2. 中華民國 TW
	住居所(中 文)	1. 台北縣板橋市溪生東路279巷12弄16-2號 2. 新竹市東區東南街289號
	住居所(英 文)	1. 2.
三、申請人(共1人)	名稱或姓 名(中文)	1. 揚智科技股份有限公司
	名稱或姓 名(英文)	1.
	國 籍(中英文)	1. 中華民國 TW
	住居所(營業所)(中 文)	1. 台北市內湖路一段246號2樓 (本地址與前向貴局申請者相同)
	住居所(營業所)(英 文)	1.
	代表人(中文)	1. 呂理達
	代表人(英文)	1.

四、中文發明摘要　（發明名稱：一種運用在無線加解密運算的硬體加速裝置）

一種運用在無線加解密運算的硬體加速裝置，包括有：複數個運算單元，每一運算單元可獨立完成一指定運算，更包括有：一資料接收裝置，兩個輸入，分別為接收外部一資料信號的一第一輸入與接收其他運算單元之一支援信號的一第二輸入，當工作模式為「普通模式」時，輸出該第一輸入，當工作模式為「加速模式」時，輸出該第二輸入；及一運算裝置，耦接該資料接收裝置，將由資料接收裝置所輸出之資料進行處理後輸出；以及一控制單元，耦接每一個運算單元，使閒置的運算單元協助運作中的運算單元處理資料，更包括有：一控制裝置，耦接每一處理單元之該資料接收裝置，發送一控制信號，以改變工作模式；及一整合裝置，耦接每一處理單元之該運算裝置及該控制裝置，整合工作模式為「加速模式」處理單元之該運算裝置的輸出。

六、英文發明摘要　（發明名稱：）

四、中文發明摘要　（發明名稱：一種運用在無線加解密運算的硬體加速裝置）

五、（一）、本案代表圖為：第 圖三 圖

（二）、本案代表圖之元件代表符號簡單說明：

1-運算單元
10-資料信號
12-資料接收裝置
121-第一輸入
122-第二輸入
13-支援信號
14-運算裝置
2-控制單元
20-控制信號
26-控制裝置
28-整合裝置

六、英文發明摘要　（發明名稱：）

一、本案已向

國家(地區)申請專利	申請日期	案號	主張專利法第二十四條第一項優先

無

二、□主張專利法第二十五條之一第一項優先權:

申請案號:

日期:

無

三、主張本案係符合專利法第二十條第一項□第一款但書或□第二款但書規定之期間

日期:

四、□有關微生物已寄存於國外:

寄存國家:

寄存機構:

寄存日期:

寄存號碼:

無

□有關微生物已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期:

寄存號碼:

無

□熟習該項技術者易於獲得,不須寄存。

五、發明說明 (1)

【發明所屬之技術領域】

本發明是關於一種運用在無線加解密運算的硬體加速裝置，尤指一種用來減少閒置(idle)狀況的發生的硬體加速裝置。

【先前技術】

近年來，隨著無線通信科技的進步，各式各樣的數位行動產品諸如手機、筆記型電腦、PDA實現了人類無線通信的願望，除了擺脫傳統有線電話的束縛，讓使用者更自由，也使人與人間的距離更近。

然而，無線網路是利用廣播(broadcast)方式在空間中傳遞。也就是說，只要有心，任何人都可以在空間中擷取到傳輸信號，得知傳輸內容，進而從事偽冒、竄改等危害網路安全的攻擊行為。特別是針對要求傳輸安全的電子商務或是機密文件的應用，更會造成極大的傷害。因此，無線傳輸信號都必需經過加密(encryption)的動作，以確保傳輸的安全。因此，美國電機電子工程學會(Institute of Electrical and Electronics Engineers, IEEE)，為了加強無線區域網路(wireless LAN, WLAN)的資料傳輸安全，特別制訂了一加密標準：IEEE 802.11i CCMP (Counter-Mode/CBC-MAC Protect)。CCMP是採用CCM(Counter-Mode with Cipher-Block Chaining Message Authentication Code, Counter-Mode with CBC-MAC)模式去控制先進加密標準

(Advance Encryption Standard, AES)。

請參閱圖一，此為CCMP的裝置圖。CCM控制邏輯接收傳輸資料，依照標準加密步驟，利用AES加密單元來完成訊息完整性檢查(message integrity check, MIC)及編解碼的運算。為加快運算速度，傳統的硬體設計上，一般會以兩個AES加密單元各自進行MIC運算及編解碼運算。並請參閱圖二，此為一封包需要MIC運算及編解碼運算之分部說明圖。無線傳輸時以封包為傳輸單位，每個封包可分為兩個部分：初始區及標頭(header)部分與承載(payload)部分，在初始區及標頭部分中，初始區為16個位元組(byte)，用以通知並初始化；標頭32個位元組，用來儲存傳輸時的必要資訊及控制碼；承載部分則為真正用來傳輸資料的部分，在無線傳輸中，為降低資料錯誤率(error rate)，一般承載部分的長度N不會太大。對於訊息完整性而言，訊息完整性檢查目的在於避免訊息遭到竄改或是部分被刪除，因此完整性輸入信號70必需包括初始區及標頭及承載兩部分，以確保訊息完整性。而對防止他人窺知資料而言，標頭部分因為不帶有所傳遞的資料，因此加解密輸入信號72只需包括承載部分及所得MIC資訊即可。

綜上所述，在傳統裝置中，會將整個完整性輸入信70送入第一AES加密單元1a，以求得MIC值，將包括承載部分及所得之MIC值的加解密輸入信號72輸入到第二AES加密單元1b，以完成加密流程。通常會以16個位元組(128個位元)為當單位，依先後順序輸入AES加密單元。然而，並不

是所有時間兩個AES加密單元都在運作，因此會有AES加密單元會出現閒置(idle)的現象，造成效能浪費。在加解密的過程中，由於運算相當複雜，瓶頸步驟通常是加解密處理步驟，因此為加快速度，必須避免閒置的現象。

【發明內容】

本發明的主要目的是提供一種硬體加速裝置，可以減少閒置(idle)，增加運算的效率。

為達上述目的，本發明提供一種運用在無線加解密運算的硬體加速裝置，包括有：

複數個運算單元，每一運算單元可獨立完成一指定運算，更包括有：

一資料接收裝置，兩個輸入，分別為接收外部一資料信號的一第一輸入與接收其他運算單元之一支援信號的一第二輸入，當工作模式為「普通模式」時，輸出該第一輸入，當工作模式為「加速模式」時，輸出該第二輸入；及

一運算裝置，耦接該資料接收裝置，將由資料接收裝置所輸出之資料進行處理後輸出；

以及

一控制單元，耦接每一個運算單元，使閒置的運算單元協助運作中的運算單元處理資料，更包括有：

一控制裝置，耦接每一處理單元之該資料接收裝置，發送一控制信號，以改變工作模式；及

一整合裝置，耦接每一處理單元之該運算裝置，整合工作模式為「加速模式」處理單元之該運算裝置的輸出。

【實施方式】

為使　貴審查委員能對本發明之特徵、目的及功能有更進一步的認知與瞭解，茲配合圖式詳細說明如後：

請參閱圖三，此為本發明之架構圖。本發明之精神在於利用閒置的處理單元支援運作中的處理單元處理資料。因此，本發明包括有：

複數個運算單元1，每一運算單元1可獨立完成一指定運算，如加密、認證或是其他的算數邏輯運算，每一運算單元1更包括有：

一資料接收裝置12，資料接收12裝置有兩個輸入，分別為接收外部一資料信號10的第一輸入121與接收其他運算單元之支援信號13的第二輸入122，當工作模式為「普通模式」時，以第一輸入121為輸出，當工作模式為「加速模式」時，以第二輸入122為輸出。資料接收裝置12可以利用一多工器實現。此外每個資料接收裝置也互相連接，以傳遞支援信號13到其他運算單元；及

一運算裝置14，耦接該資料接收裝置12，將由資料接收裝置21所輸出之資料進行如算數邏輯運算等處理後輸出；

以及

一控制單元2，耦接每一個運算單元1，使閒置的運算單元1能夠支援運算，以協助運作中的運算單元1處理資料，更包括有：

一控制裝置26，耦接每一處理單元1之該資料接收裝置，發送一控制信號20，以改變工作模式；及

一整合裝置28，耦接每一處理單元之該運算裝置26及該控制裝置26，將工作模式為「加速模式」處理單元1所輸出的信號加以整合，也就是將交由其他運算單元1處理的結果與運算中運算單元1處理的結果，加以整合。

請參閱圖四，此為本發明之一具體實施例。這是一個運用在CCMP安全協定的實施例。在本實施例中，包括兩個AES加密單元1a、1b，每個AES加密單元的輸入是128位元，但是在一個單位時間內，AES加密單元每次只能處理32位元，因此需要一個雙字組選擇邏輯(double word selection logic)將一個128位元的輸入分成四個32位元的輸入，以逐次處理。因此，在這個實施例中，資料接收裝置12就為雙字組選擇邏。控制單元2監測兩個運算單元1a、1b的運作狀況，當偵測到第二AES運算單元1b閒置時，控制單元2之控制裝置26就將一控制信號20送入第二AES運算單元1b，將工作模式由「普通模式」改成「加速模式」以協助工作中的第一運算單元1a加速運算。此時，第一AES運算單元1a就可以把支援信號13從雙字組選擇邏輯送到「加速模式」的第二AES單元1b。支援信號13的傳

送除可運算單元間另外架構資料傳輸線，利用該資料傳輸線傳遞外，也可以經由控制裝置26轉送。本實施例中，運算單元1間的支援信號13乃是利用控制裝置26轉送，所以不需增加其他線路。當第二AES運算單元1b，接收由工作中的運算單元送過來的支援信號13後，開始以「加速模式」對支援信號13進行加解密運算，所得到的結果，需彙整到整合裝置28，由整合裝置28根據控制裝置26的控制信號20，將處於「加速模式」的第二AES運算單元1b的輸出與第一AES運算單元1a的輸出作一整合性的處理後，方能輸出。本實施例中，整合裝置28可直接跨接該運算裝置，以直接之取得輸出，並且也不影響在「普通模式」時的輸出。

綜上所述，一個128bit的資料會被分成4個32bit的輸入，在第二AES運算位元1b閒置時，可以將其中兩個32bit的輸入交由該第二AES運算位元1b處理，以增進效率及加快處理時間。由於加解密的運算相當繁複，目前的標準作法是一個輸入要在AES加密單元運算十次才會輸出，因此本發明的作法在實際上將可以節省許多運算時間。本發明除了以32 bit的資料為單位外，也可以一個訊框(frame)或是其他為單位輸入閒置的運算單元以增加運算效率。

唯以上所述者，僅為本發明之較佳實施例，當不能以之限制本發明的範圍。即大凡依本發明申請專利範圍所做之均等變化及修飾，仍將不失本發明之要義所在，亦不脫離本發明之精神和範圍，故都應視為本發明的進一步實施

五、發明說明 (7)

狀況。

【圖式簡單說明】

圖一係為CCMP的裝置圖

圖二係為封包需要MIC運算及編解碼運算之分部說明圖

圖三係為本發明之架構圖

圖四係為本發明之一具體實施例

圖號說明：

1-運算單元

1a-第一AES運算單元

1b-第二AES運算單元

10-資料信號

12-資料接收裝置

121-第一輸入

122-第二輸入

13-支援信號

14-運算裝置

2-控制單元

20-控制信號

26-控制裝置

28-整合裝置

70-完整性輸入信號

72-加解密輸入信號

六、申請專利範圍

1. 一種運用在無線加解密運算的硬體加速裝置，包括有：

複數個運算單元，每一運算單元可獨立完成一指定運算，更包括有：

一資料接收裝置，兩個輸入，分別為接收外部一資料信號的一第一輸入與接收其他運算單元之一支援信號的一第二輸入，當工作模式為「普通模式」時，輸出該第一輸入，當工作模式為「加速模式」時，輸出該第二輸入；及

一運算裝置，耦接該資料接收裝置，將由資料接收裝置所輸出之資料進行處理後輸出；

以及

一控制單元，耦接每一個運算單元，使閒置的運算單元協助運作中的運算單元處理資料，更包括有：

一控制裝置，耦接每一處理單元之該資料接收裝置，發送一控制信號，以改變工作模式；及

一整合裝置，耦接每一處理單元之該運算裝置及該控制裝置，整合工作模式為「加速模式」處理單元之該運算裝置的輸出。

2. 如申請專利範圍第1項所述之運用在無線加解密運算的硬體加速裝置，其中該資料接收裝置可為一多工器。

3. 如申請專利範圍第1項所述之運用在無線加解密運算的硬體加速裝置，其中該資料接收裝置可為一雙字組選擇邏輯(double word selection logic)。

4. 如申請專利範圍第1項所述之運用在無線加解密運算的

六、申請專利範圍

硬體加速裝置，其中該運算單元可為先進加密標準(Advance Encryption Standard, AES)之運算單元，該指定運算為AES運算。

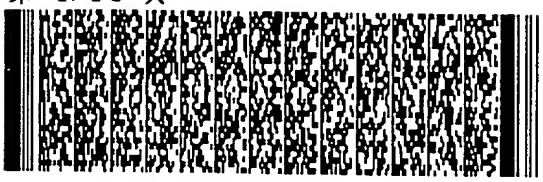
5. 如申請專利範圍第1項所述之運用在無線加解密運算的硬體加速裝置，其中該加速裝置可包括兩個AES之運算單元。

6. 如申請專利範圍第1項所述之運用在無線加解密運算的硬體加速裝置，其中該控制裝置更連接到每一個處理單元之運算裝置，以確認該運算裝置是否為閒置狀態。

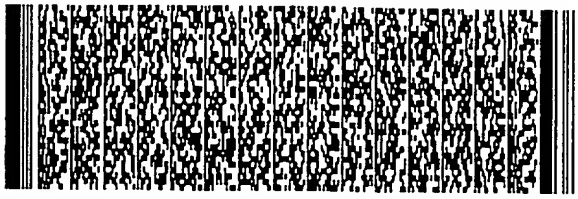
7. 如申請專利範圍第1項所述之運用在無線加解密運算的硬體加速裝置，其中該控制裝置可轉送資料。

8. 如申請專利範圍第1項所述之運用在無線加解密運算的硬體加速裝置，其中該整合裝置可跨接該運算裝置之輸出。

第 1/14 頁



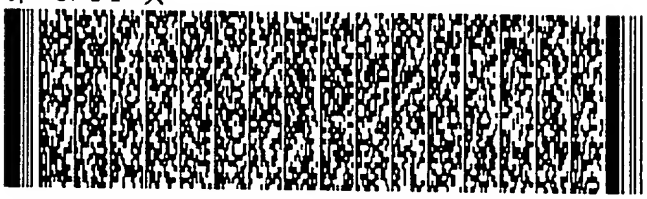
第 2/14 頁



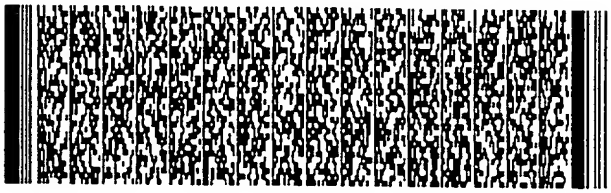
第 3/14 頁

第 4/14 頁

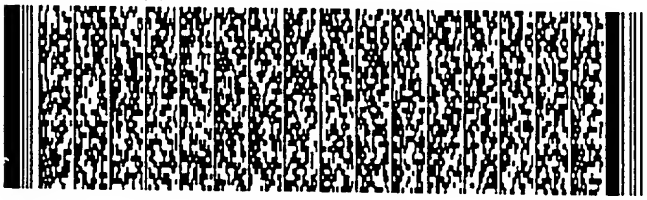
第 5/14 頁



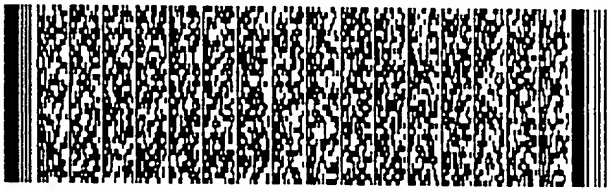
第 5/14 頁



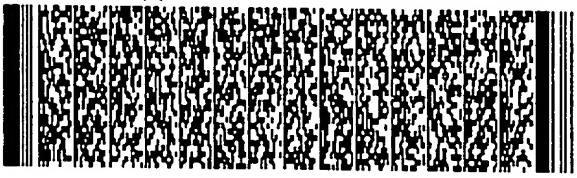
第 6/14 頁



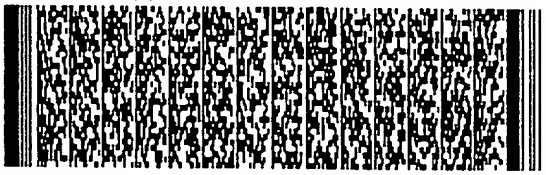
第 6/14 頁



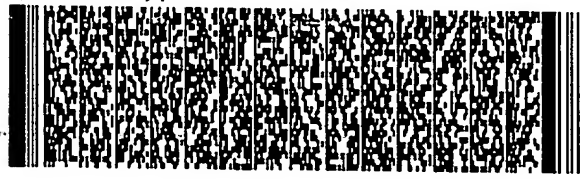
第 7/14 頁



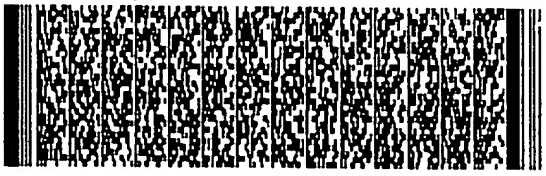
第 7/14 頁



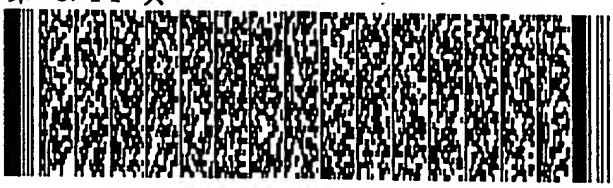
第 8/14 頁



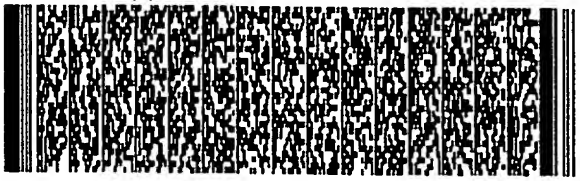
第 8/14 頁



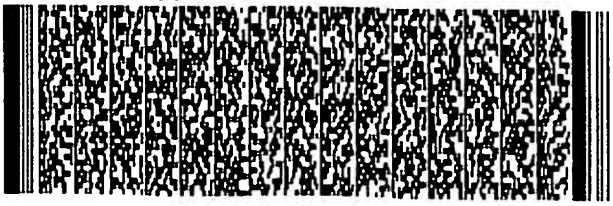
第 9/14 頁



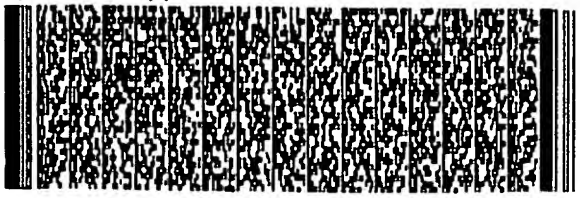
第 9/14 頁



第 10/14 頁

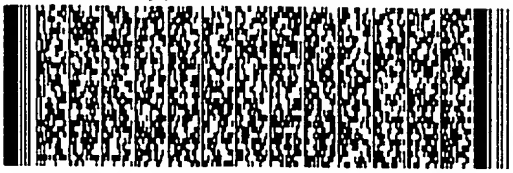


第 10/14 頁

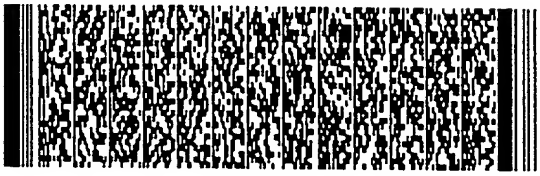


第 11/14 頁

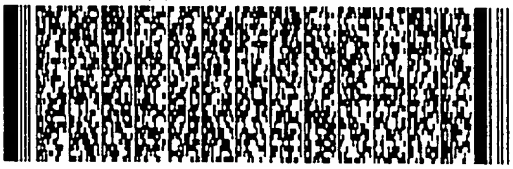
第 12/14 頁



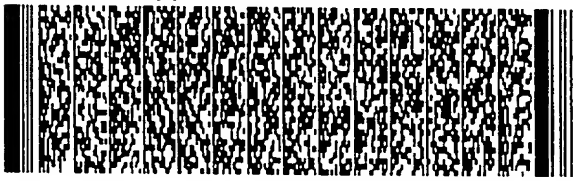
第 13/14 頁



第 13/14 頁



第 14/14 頁



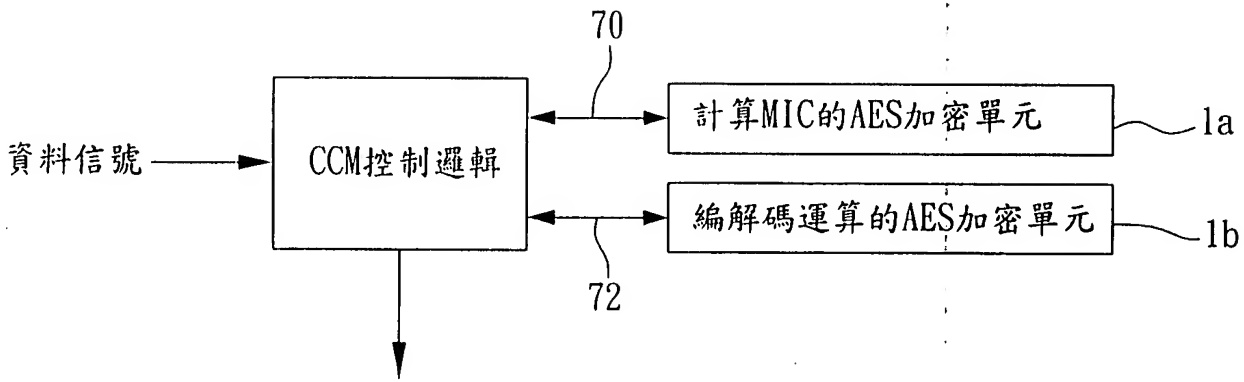


圖 一

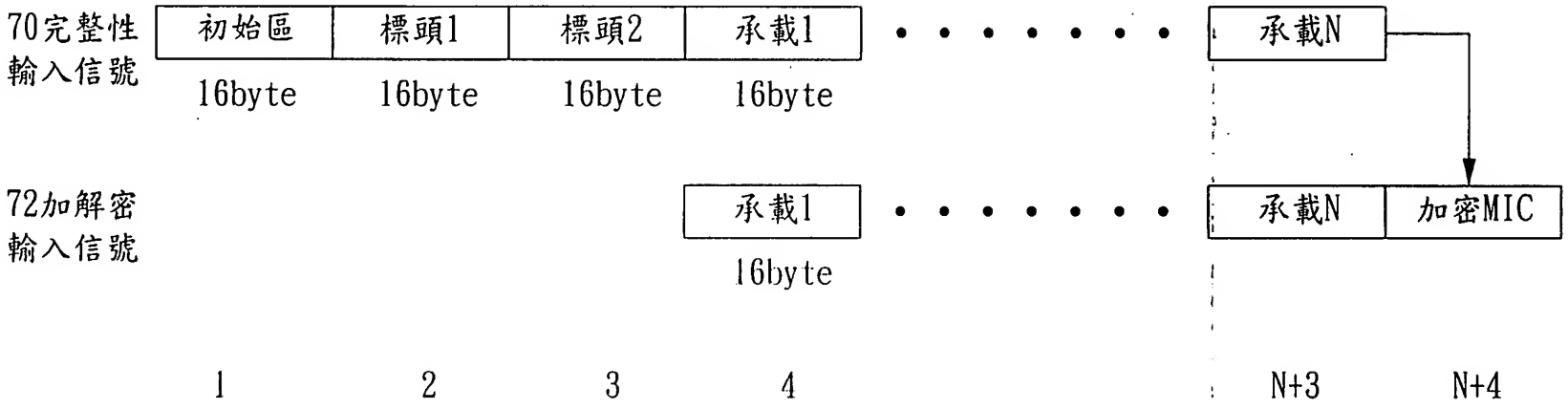

70完整性
輸入信號
初始區
標頭1
標頭2
承載1
承載N
16byte
16byte
16byte
16byte
72加解密
輸入信號
承載1
承載N
加密MIC
16byte
1
2
3
4
N+3
N+4

圖 二

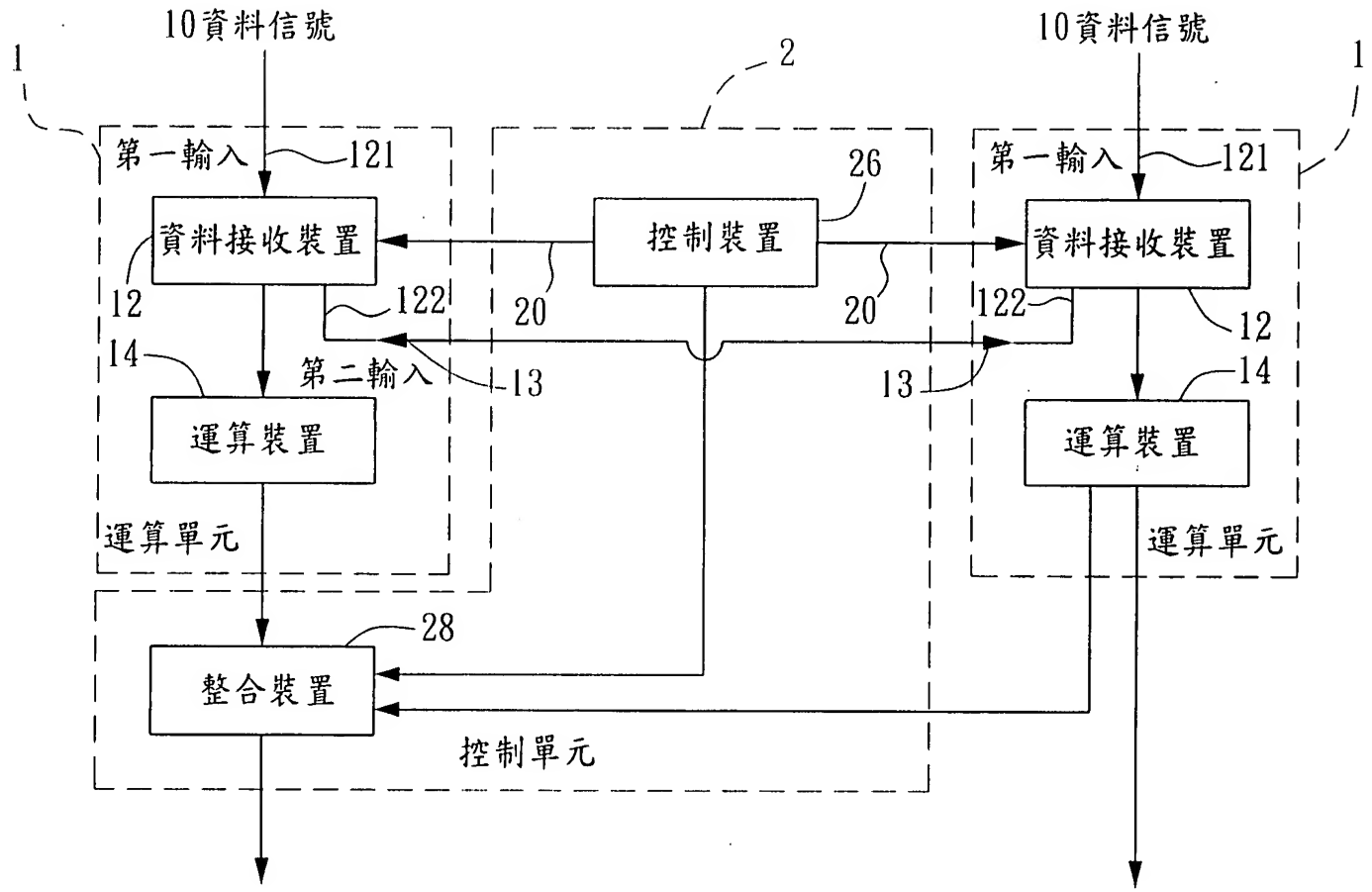

10資料信號
1
2
10資料信號
1
第一輸入
121
26
第一輸入
121
資料接收裝置
控制裝置
資料接收裝置
12
122
20
20
122
12
14
第二輸入
13
13
14
運算裝置
運算裝置
運算單元
運算單元
28
整合裝置
控制單元

圖 三

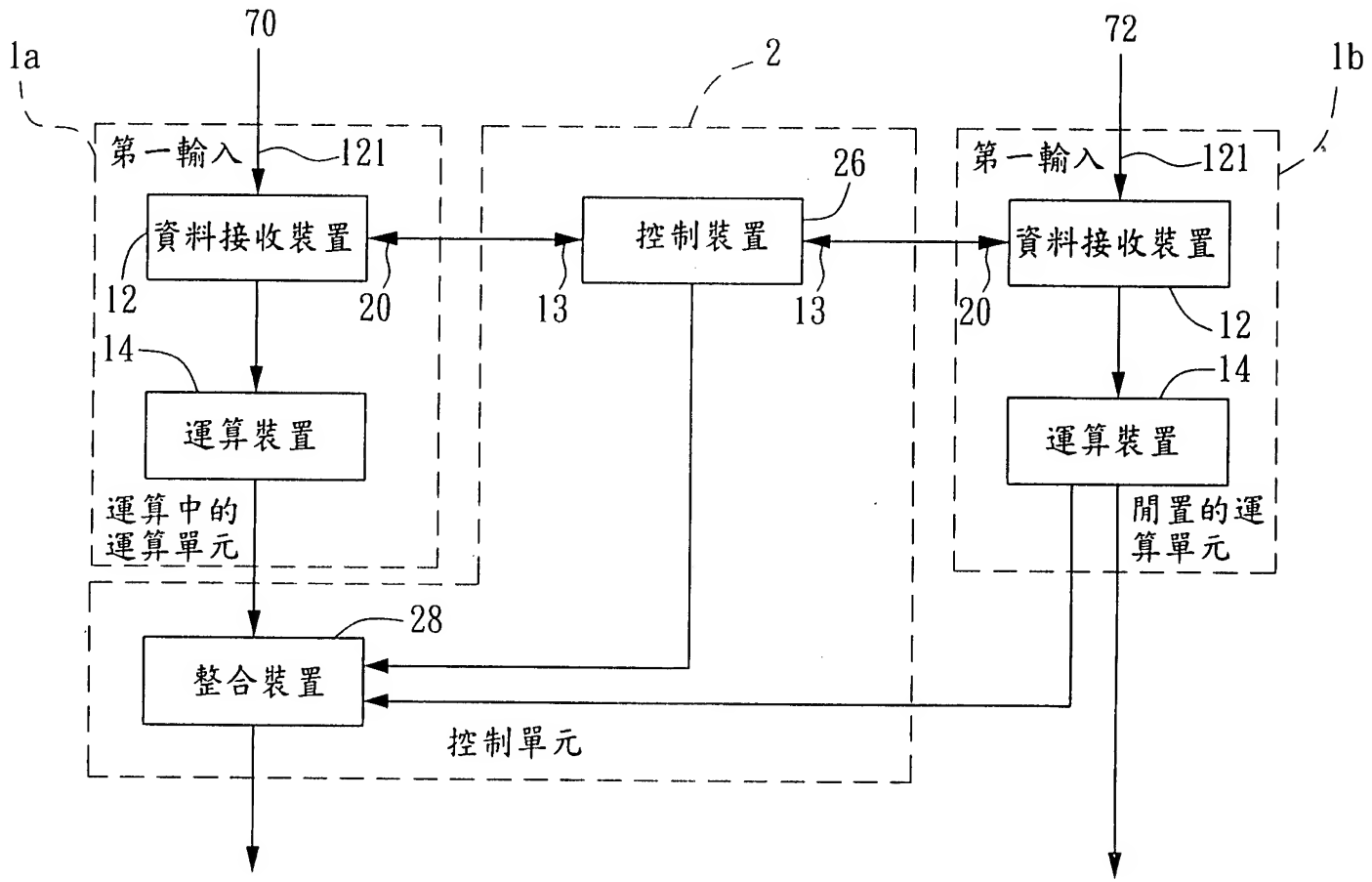

70
72
1a
2
1b
第一輸入
121
第一輸入
121
26
資料接收裝置
控制裝置
資料接收裝置
12
20
13
13
20
12
14
14
運算裝置
運算裝置
運算中的
運算單元
閒置的運
算單元
28
整合裝置
控制單元

圖 四